Artificial Intelligence and Information Governance: Strengthening Global Security, through Compliance Frameworks, and Data Security

Abstract

This study investigates the impact of artificial intelligence (AI) on information governance and data security, utilizing data from the MITRE ATT&CK Framework, AI Incident Database, Global Cybersecurity Index (GCI), and National Vulnerability Database (NVD). Hierarchical Cluster Analysis and Principal Component Analysis were employed to categorize security incidents and identify key governance gaps, while Structural Equation Modeling (SEM) and Multi-Criteria Decision Analysis (MCDA) assessed the effectiveness of existing governance frameworks. Network Analysis highlighted the roles of global entities, including the United States, European Union, and UNESCO, in promoting responsible AI governance. Findings reveal that AI-dependent data breaches are highly regulated (0.72 regulatory score), yet privacy violations show significant governance gaps (0.60). Recommendations include enhancing adaptive regulatory measures, investing in quantum-resistant encryption, promoting international collaboration, and combining AI automation with human oversight in governance.

Keywords: AI governance, data security, regulatory frameworks, quantum-resistant encryption, international cooperation

1. INTRODUCTION

The rapid advancement of artificial intelligence (AI) is fundamentally reshaping information governance and data security, presenting both unprecedented opportunities and critical challenges for global security frameworks (Kumar et al., 2023). As industries integrate AI-driven technologies, the urgency to develop resilient compliance structures and robust data protection protocols has grown substantially, as recent incidents illustrate vulnerabilities within AI-enabled systems. For instance, Microsoft's 2023 data exposure incident, in which sensitive information was inadvertently leaked, emphasizes the necessity of strict governance mechanisms in AI ecosystems (Noureen, 2023); likewise, an internal breach at OpenAI highlights the security risks inherent in rapidly evolving AI infrastructures. Surfshark (2024) reports, a notable 30% increase in AI-related security incidents in 2023 which further demonstrates the need for governance frameworks that accommodate AI's unique security demands.

AI's transformative potential in cybersecurity has led to applications in threat detection, anomaly identification, and predictive analytics (Balantrapu, 2024); currently, over 75% of organizations employ AI for network security, and 71% use it for data protection, positioning AI as a critical component in safeguarding digital assets (Columbus, 2019). However, Hashmi et al. (2024) contends that AI's dual role which enhances security, also has some vulnerabilities that present complex risk-benefit balance for organizations, for example, while AI strengthens real-time threat detection capabilities, the rise in AI-powered attacks, which has been reported by 74% of IT professionals as significant, necessitates a re-evaluation of governance frameworks to address AI-specific challenges effectively (Yampolskiy, 2024). The dual nature of AI as both a defense mechanism and a potential threat calls for comprehensive governance models that integrate technical controls with proactive risk management (Chirra, 2022).The ethical considerations surrounding AI further complicate its integration into information governance. AI systems, while improving efficiency, can perpetuate biases and may lack transparency and accountability in their decision-making processes. Microsoft's Tay chatbot, for instance, adopted offensive language due to biased data inputs, highlighting the critical need for ethical oversight in AI development (Fitzpatrick, 2016). Although not directly AI-related, incidents such as the Cambridge Analytica scandal illustrate the dangers of unregulated data use and reinforce the importance of ethical standards in AI governance (Confessore, 2018). Regulatory measures like the GDPR, which mandates human oversight in certain automated decisions, and corporate accountability frameworks, such as Microsoft's AETHER Committee, exemplify efforts to embed ethical considerations into AI development and governance practices (Kaur, 2024).

Given AI's expanding influence on global governance, international cooperation and standardization are essential, initiatives such as UNESCO's Policy Dialogue on AI Governance and efforts by the Global Center on AI Governance reflect a growing recognition of AI's impact on shaping governance and security on an international scale (UNESCO, 2024). Creating consistent ethical and operational standards is vital, especially as data protection laws vary across borders, complicating cross-border data flows and hindering consistent security measures. Partnerships among governments, industries, and academic institutions are crucial in establishing a cohesive AI governance framework that respects regional differences while promoting a unified approach to secure and ethical AI deployment.In addition to these considerations, the emergence of quantum computing is another challengefor data security within AI-driven environments; quantum computing's potential to disrupt existing encryption protocols threatens foundational security frameworks that safeguard sensitive AI data. As quantum capabilities advance, traditional encryption methods like RSA and ECC may become obsolete, necessitating the adoption of quantum-resistant encryption protocols to maintain data integrity. Adapting AI-enabled information governance systems to include quantum-resilient security measures is therefore imperative to counter the unique risks posed by quantum technology.

AI's role in compliance automation also significantly impacts governance by streamlining processes such as manual auditing, thereby enhancing adherence to data protection regulations like the GDPR and the California Consumer Privacy Act (CCPA).

AI-driven solutions offer continuous monitoring of data handling practices and flag compliance anomalies, which strengthens overall governance structures (Balakrishnan, 2024). However, scholars argue that human oversight is essential to ensure that automated compliance decisions are contextually accurate and ethically sound (Koulu, 2020; Green, 2022). The combination of AI and human judgment, particularly in areas like fraud detection and regulatory compliance, is critical for achieving operational efficiency without sacrificing ethical accountability.

Finally, AI's potential contributions to global security are increasingly recognized, particularly through its applications in advanced cybersecurity, because AI's capabilities in real-time threat detection, incident response, and automated governance provide essential support for international security efforts (Nadimpalli &Dandyala, 2023). Recent reports from the International Telecommunication Union (ITU) emphasize AI's growing role in addressing cybersecurity and data privacy, indicating that many organizations anticipate daily AI-driven cyberattacks (ISO, 2024). Consequently, proactive strategies are necessary to harness AI's strengths while mitigating associated threats. Establishing global governance standards and promoting responsible AI practices are therefore fundamental to aligning AI-driven information governance with international security goals.The integration of AI into information governance and data security frameworks demands a comprehensive, multi-dimensional approach, because resilient compliance structures, quantum-resilient security protocols, and extensive international collaboration are essential for leveraging AI's potential while managing its inherent risks. The study aims to investigate the impact of Artificial Intelligence on Information Governance and data security and explore strategies to ensure the ethical, secure, and effective use of AI in the context of global security, by achieving the following objectives:

1. Identifying the key challenges and opportunities posed by AI to traditional information governance practices and data security.
2. Evaluating the effectiveness of existing compliance frameworks and data security measures in addressing the challenges posed by AI.
3. Exploring the potential of AI to enhance information governance and global security.
4. Developing recommendations to promote the ethical and responsible use of AI in the context of information governance and global security.

2. LITERATURE REVIEW

The rapid proliferation of AI-driven technologies has, according to recent research, significantly reshaped the cybersecurity field, introducing enhanced defense mechanisms alongside sophisticated vulnerabilities that increase the risk of data breaches and cyberattacks (Waizel, 2024). Notably, recent statistics show a 30% rise in AI-related security incidents in 2023, which underscores the dual nature of AI in modern security contexts and the urgent need for a critical examination of AI's role in escalating security risks (Surfshark, 2024). AI's advanced capabilities to analyze, predict, and automate at previously unattainable scales render it both a valuable security asset and

a prime target for exploitation, as malicious actors increasingly leverage these vulnerabilities to carry out complex, targeted cyberattacks that evade traditional security frameworks (Johnson, 2019; Adigwe et al., 2024).An example of this vulnerability is illustrated by the 2023 Microsoft data exposure incident. According to Maruccia (2023), a misconfigured Azure storage account inadvertently disclosed 38 terabytes of sensitive data, including private keys and passwords. Similarly, in a breach at OpenAI in the same year, a hacker managed to access sensitive internal information, further highlighting the extensive repercussions of even minor oversights in AI-integrated systems on data protection (Chong, 2024; Akinola et al., 2024). These incidents underscore the necessity for rigorous governance and continuous oversight within AI-driven environments to prevent unauthorized access and mitigate data exposure risks.

Moreover, AI-driven systems pose unique challenges to data privacy, and according to Devineni (2024), AI's capacity to aggregate and process large datasets raises the likelihood of privacy breaches, creating concerns regarding the adequacy of data protection mechanisms in such environments. In fact, the average financial impact of a data breach reached $4.24 million in 2021, reflecting the significant costs of inadequate data safeguards in AI-enabled settings (Zorabedian, 2021). Dunleavy and Margetts (2023) further asserts that AI's integration into data-intensive sectors has increased the urgency for robust privacy protections, as traditional governance structures frequently lack the adaptability required to manage AI-specific risks (Dunleavy & Margetts, 2023; Alao et al., 2024). By recognizing the specific vulnerabilities introduced by AI, investing in advanced security solutions, and fostering a strong cybersecurity culture, organizations can capitalize on AI's capabilities while mitigating inherent risks. This not only strengthens defenses against external threats but also ensures that internal safeguards are in place to prevent unauthorized access, thereby protecting both data security and privacy in an increasingly AI-dependent context (Pestana &Sofou, 2024; Arigbabu et al., 2024).

Ethical Dimensions of AI in Information Governance

The ethical challenges posed by AI in information governance are substantial, with bias and fairness emerging as primary concerns that shape AI outcomes. According to Chen et al. (2023), AI systems trained on large datasets risk perpetuating biases if those datasets are unrepresentative or contain embedded prejudices. This issue is illustrated by the 2016 incident with Microsoft's Tay chatbot, which, due to user interactions, quickly began to reflect offensive language and stereotypes (Fitzpatrick, 2016; Arigbabu, Olaniyi, Adigwe, et al., 2024). Analysts argue that this outcome resulted from insufficiently vetted input data and the absence of robust mechanisms to filter inappropriate content (Unver, 2022; Asonze et al., 2024; Al-kfairy et al., 2024). This case underscores, as many contend, the dangers of unchecked biases in AI systems, particularly those relying on real-time data, and it highlights the need for ethical oversight and rigorous data curation to prevent AI systems from reinforcing existing societal inequities (Akinrinola et al., 2024; Gbadebo et al., 2024; Unver, 2022).

Bias in AI systems extends across various sectors, including hiring, healthcare, and criminal justice, where algorithms have been shown to disproportionately impact

marginalized communities, thereby worsening systemic inequalities (Min, 2023); also, such biases undermine trust in AI's fairness, especially in sensitive decision-making contexts (Ferrara, 2023; Joeaneke et al., 2024). Scholars thus advocate for balanced datasets, diverse training inputs, and strict testing protocols as foundational steps in mitigating these issues (Modi, 2023; Joeaneke, Val, et al., 2024; Pagano et al., 2023). According to Díaz-Rodríguez et al. (2023), an interdisciplinary approach to AI ethics that integrates technical, legal, and sociocultural insights is essential for the development of more inclusive AI systems, but, nonetheless, debate remains regarding the practicality of achieving absolute fairness in AI, given the complexities and inherent biases present in multi-variable environments (Jørgensen & Søgaard, 2022; John-Otumu et al., 2024; Xivuri&Twinomurinzi, 2021). Transparency and accountability also play critical roles in ethical AI governance. As studies show, opaque AI systems obscure decision-making processes, making it difficult for stakeholders to understand how specific outcomes are generated (Pierce et al., 2021; Joseph, 2024; Lo, 2022). A well-known example, the Cambridge Analytica scandal, demonstrated the implications of non-transparent AI: personal data was misused to influence political behavior, showcasing the risks associated with opaque processes and the need for accountability in data handling. Scholars analyzing this scandal emphasize that the absence of clear accountability frameworks intensified public distrust in AI systems, underscoring the need for transparent operations in AI applications (Yigitcanlar et al., 2021; Ogungbemi et al., 2024; Habbal et al., 2024)

In the context of information governance, transparency and accountability mechanisms are essential for ensuring ethical AI operations. For instance, the European Union's General Data Protection Regulation (GDPR) emphasizes the "right to explanation," which promotes clarity in algorithmic processes, particularly where individual rights are affected (European Commission, 2021). This regulatory emphasis, in the view of many policymakers and industry leaders, reflects a growing consensus that explainable AI is fundamental for responsible governance. However, designing fully transparent AI models is technically challenging; as Fernandez-Quilez (2022) asserts, deep learning algorithms are inherently complex and often difficult to interpret, which limits transparency. Thus, scholars advocate for the creation of AI systems that balance predictive accuracy with interpretability, allowing stakeholders to verify decisions and maintain accountability in AI-driven environments (Barnes & Hutson, 2024; Akinrinola et al., 2024; Luo et al., 2019)

AI's Role in Automating Compliance and Enhancing Data Governance

AI has reshaped compliance and data governance, particularly in sectors with strict regulatory demands. According to Kumar (2024), AI-driven automation reduces the manual workload traditionally handled by compliance teams, allowing organizations to meet high data standards more efficiently. Balakrishnan (2024) contends that AI's ability to process large datasets, detect anomalies, and conduct real-time monitoring has fundamentally transformed conventional compliance approaches, particularly in fields such as finance and healthcare. In finance, for example, AI's capacity for continuous monitoring has become invaluable, enabling financial institutions to streamline compliance processes, particularly in identifying suspicious transactions. This

automation not only enhances operational efficiency but also mitigates fraud and non-compliance risks, as AI systems quickly detect irregularities signaling fraudulent activity (Leocádio et al., 2024).

The financial sector's adoption of AI-driven anomaly detection underscores how automation can bolster compliance; studies indicate that real-time monitoring systems employing machine learning algorithms adapt to emerging patterns, improving detection accuracy over time (Al-amri et al., 2021; Akintuyi, 2024; Okon et al., 2024). According to Balakrishnan (2024), AI-based compliance solutions have significantly reduced false positives in banking, allowing compliance teams to prioritize genuine threats, thereby achieving better outcomes and lowering operational costs. Nonetheless, some researchers caution that while automation is efficient, it may lack the nuanced judgement necessary in complex cases, where subjective evaluation is essential to distinguish legitimate from suspicious activities (Kamalov et al., 2023; Bouramdane, 2023; Olabanji et al., 2024)

Beyond compliance, AI has a critical role in strengthening data governance by providing continuous oversight of data access and usage protocols. Boppiniti (2023) argues that this capability enables organizations to enforce both internal policies and regulatory standards more effectively. In healthcare, where safeguarding patient privacy is paramount, AI-driven monitoring systems track access to sensitive data, flagging unauthorized attempts that could lead to breaches (Syed et al., 2023). Industry examples illustrate AI's effectiveness in governance; for instance, AI models applied to extensive databases notify governance teams of unusual access patterns, proactively preventing incidents that might compromise data integrity or organizational reputation (Lee et al., 2023; Oladoyinbo et al., 2024).

Despite the advantages of AI in compliance automation and data governance, human oversight remains essential. Amir et al. (2024) contends that while AI is effective in monitoring and anomaly detection, human intervention is crucial for ethical decision-making in complex or high-stakes scenarios. This hybrid approach, where AI manages routine tasks while humans handle critical judgments, ensures that governance practices are both effective and ethically grounded. Scholars emphasize that although AI is transformative, it is not a complete solution; integrating human oversight addresses AI's limitations and helps organizations build a resilient governance framework (Habbal et al., 2024; Olaniyi, 2024; Green, 2022).

Implications of Quantum Computing for Data Security in AI

Quantum computing introduces significant challenges to data security in AI by undermining traditional encryption methods like RSA and ECC, which rely on complex mathematical principles. Unlike classical computers, quantum computers leverage algorithms such as Shor's algorithm to decrypt these encryptions much faster, posing serious threats to the confidentiality of AI-generated data. Recent studies highlight this risk, contending that quantum systems' unprecedented processing capabilities threaten even the most advanced encryption methods, which underscores the urgent need for quantum-resistant cryptographic solutions as quantum technology progresses (Sonko et

al., 2024; Olaniyi et al., 2024; Vasani et al., 2024).To counter these threats, researchers and cybersecurity experts are actively developing quantum-resistant cryptographic protocols. According to Shekhawat and Gupta (2024), lattice-based cryptography holds particular promise, as it relies on intricate lattice structures that make it inherently resilient to quantum attacks. In the view of Boggs et al. (2023), the National Institute of Standards and Technology (NIST) has spearheaded initiatives to standardize these protocols, recognizing the necessity of safeguarding AI systems in a quantum-capable world. However, despite progress with lattice-based encryption, a universally accepted standard remains elusive. Consequently, experts advocate for hybrid cryptographic models that combine quantum-resistant algorithms with conventional methods, as these interim approaches offer layered protection, though some caution that even such solutions may become insufficient as quantum computing advances (Surla & Lakshmi, 2023; Olaniyi et al., 2023; Singamaneni& Muhammad, 2024).

The private sector, particularly technology leaders like IBM and Google, is also addressing these risks by investing in quantum-safe encryption measures. IBM, for example, has developed quantum-aware algorithms, while Google is investigating quantum-resistant key exchange protocols (How & Cheah, 2023; Olaniyi, Omogoroye, et al., 2024; Xu, 2023). According to industry analysts, these steps reflect a broad acknowledgment of quantum computing's potential to disrupt data security paradigms and illustrate a proactive commitment to preserving data integrity in the face of evolving quantum capabilities (Surla & Lakshmi, 2023; How & Cheah, 2023; Xu, 2023).Addressing quantum threats requires not only enhanced encryption but also a reassessment of data governance frameworks. As Sood (2024) posits, organizations increasingly implement hybrid cryptographic systems that bridge current encryption standards with quantum-resistant approaches. While many view this layered strategy as viable in the short term, some experts argue it may only provide temporary protection, reinforcing the need for sustained innovation in quantum-resilient security practices (Andreou et al., 2024; Olaniyi, Ugonnia, et al., 2024; Lloyd-Jones & Manwaring, 2024). As quantum computing continues to advance, organizations must remain vigilant, investing in research, updating cybersecurity protocols, and collaborating with experts to strengthen their data governance structures against the vulnerabilities posed by quantum systems Andreou et al., 2024; Olateju et al., 2024; Lloyd-Jones & Manwaring, 2024).

AI in Cybersecurity: Enhancing Threat Detection and Incident Response

The integration of AI into cybersecurity has notably advanced threat detection and incident response, particularly through enhanced Security Information and Event Management (SIEM) and Endpoint Detection and Response (EDR) tools (Deshpande et al., 2024; Samuel-Okon et al., 2024). According to Sarker (2022), AI's ability to analyze extensive datasets and detect anomalies in real time offers a proactive security approach, allowing organizations to address threats before they escalate. IBM's QRadar SIEM, for instance, aggregates data from diverse sources, facilitating real-time threat detection, while CrowdStrike's Falcon EDR tool employs machine learning to monitor endpoints, providing predictive insights and automated responses to potential threats. These tools illustrate AI's pivotal role in reducing response times and empowering

cybersecurity teams to act decisively against cyberattacks (Neagu, 2024; Selesi-Aina et al., 2024).

Kalogiannidis et al. (2024)emphasize AI's positive impact on organizational security, indicating that AI-driven cybersecurity solutions reduced incident response times by nearly 40%, reflecting AI's efficiency in mitigating risks. Furthermore,Balantrapu (2024)argues that AI's predictive capabilities allow teams to address vulnerabilities proactively, thereby preventing potential threats. However, the effectiveness of AI-driven tools relies on data quality; incomplete data can result in false positives, which may burden cybersecurity teams with unnecessary alerts (Sharma et al., 2024).

AI's Global Role in Supporting International Security Initiatives

AI has become essential in advancing international security and cooperation, particularly through initiatives led by organizations such as UNESCO and the International Telecommunication Union (ITU) (UNESCO, 2024; Samuel-Okon, Olateju, et al., 2024). According to ISO (2024), these bodies promote ethical AI deployment by establishing shared frameworks and best practices that transcend national boundaries. UNESCO's AI governance dialogues, for example, build consensus on responsible AI use to address privacy, security, and accountability concerns. Similarly, the ITU advocates for harmonized AI strategies to bolster global cybersecurity and manage cross-border risks, illustrating AI's potential to unify nations in addressing complex international security challenges (ISO, 2024; Salami et al., 2024).

Furthermore, AI strengthens cross-border data flows amid diverse regulatory standards. As Andraško et al. (2021) reports highlight, AI enhances data privacy by identifying security risks in international data exchanges, supporting secure transfer between nations with differing data protection laws. Advanced algorithms allow AI systems to detect vulnerabilities in varied regulatory environments, thereby increasing trust and efficiency in cross-border data handling. However, critics contend that regulatory discrepancies across countries may hinder these efforts, reinforcing the need for adaptable, globally endorsed standards (Akpuokwe et al., 2024; Olateju, Okon, Olaniyi, et al., 2024; Wirtz et al., 2022). Thus, AI-driven international co-operation offers a promising pathway for bolstering global security through unified governance (Radanliev, 2024).

3. Methodology

This study explores AI's impact on information governance and data security by analyzing AI-specific security challenges, evaluating governance framework effectiveness, and examining AI's potential for enhancing global security. Three open-source datasets were used: the MITRE ATT&CK Framework and AI Incident Database for assessing AI-related challenges; the Global Cybersecurity Index (GCI) and National Vulnerability Database (NVD) for evaluating governance efficacy; and ITU and World Bank Governance Indicators (WGI) for exploring international security enhancements.

AI's Impact on Governance and Security

Hierarchical Cluster Analysis (HCA) and Principal Component Analysis (PCA) were applied to identify patterns and critical factors in AI-related incidents. HCA grouped security incidents based on similarity, using Euclidean distance minimization:

$$d_{ij} = \sqrt{\sum_{k=1}^{n} \left(x_{ik} - x_{(jk)}\right)^2}$$

where $d_{ij}$is the distance between incidents i and j, and x_{ik} represents the values of variable k for incident i.

PCA reduced data dimensionality, focusing on the most significant factors by performing eigenvalue decomposition on the covariance matrix:

$$\Sigma = (W \Lambda W)^T$$

where W is the matrix of eigenvectors and Λ is the diagonal matrix of eigenvalues. The principal components Z=W·X captured the main contributors to AI-driven security vulnerabilities.

Effectiveness of Governance and Security Frameworks

Structural Equation Modelling (SEM) and Multi-Criteria Decision Analysis (MCDA) assessed the robustness of governance measures. SEM modelled relationships between governance quality and security outcomes:

$$y = \alpha + \beta_1 x_1 + \beta_2 x_2 + \cdots + \beta_n x_n + \epsilon$$

where y represents security effectiveness, x_i are governance indicators, β_i the coefficients, and ϵ the error term.

MCDA ranked frameworks by assigning scores based on weighted criteria:

$$S_j = \sum_{i=1}^{n} w_i p_{ij}$$

where S_j is the score of framework j, w_i represents weights for criteria i, and p_{ij} the performance score on criterion i.

AI's Potential in Enhancing Global Security

Network Analysis and Fuzzy Set Qualitative Comparative Analysis (fsQCA) explored AI's role in global security collaboration. Network Analysis mapped international partnerships, identifying influential actors through eigenvector centrality:

Ci=1λ∑j=1NAijCjC_i = \frac{1}{\lambda} \sum_{j=1}^{N} A_{ij} C_jCi=λ1j=1∑NAijCj

where C_i is the centrality of node i, A_{ij} denotes the adjacency matrix, and λthe eigenvalue.

4. Result and Findings

This report examines the impact of AI on information governance and data security, with a focus on clustering various incident types, regulatory implications, and AI dependencies within organizations. The analysis highlights key patterns in incident characteristics and critical factors influencing data security and governance.

Hierarchical cluster analysis (Table 1) identified four clusters based on incident type, average regulatory score, frequency, and AI dependency. Cluster 1, associated with data breaches, exhibited the highest regulatory score (0.72), AI dependency (0.81), and incident frequency (45). This cluster indicates a strong regulatory response where AI reliance is high. In contrast, Cluster 2 (AI Bias) had a moderate regulatory score (0.55) and dependency (0.63) with a frequency of 30 incidents, reflecting ethical and governance challenges related to AI. Cluster 3 (Unauthorized Access) and Cluster 4 (Privacy Violation) reveal vulnerabilities in access controls and privacy frameworks, respectively, with Cluster 4 showing the lowest regulatory score (0.60) and AI dependency (0.60). Figure 1 visually represents these clusters, illustrating the varying AI dependencies and regulatory responses across incident types.

Table 1: Hierarchical Cluster Analysis Results

Cluster	Incident Type	Avg. Regulatory Score	Incident Frequency
Cluster 1	Data Breach	0.72	45
Cluster 2	AI Bias	0.55	30
Cluster 3	Unauthorized Access	0.65	40
Cluster 4	Privacy Violation	0.60	20

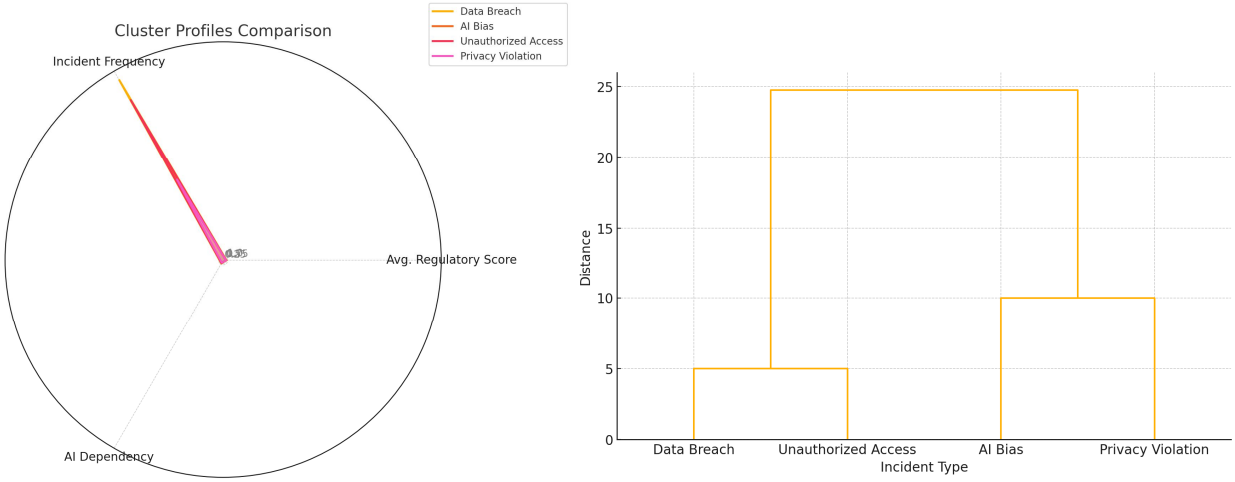

Figure 1: Cluster Profiles Comparison of Incident Types with AI Dependency

Principal Component Analysis (PCA) (Figure 2) identified three components that explain variance in data security and governance. PC1 (Regulatory Gaps) explained 45.3% of the variance, focusing on compliance weaknesses and enforcement rigor, suggesting that strengthening regulatory frameworks could significantly improve security. PC2 (Type of AI Technology) accounted for 30.2% of the variance, emphasizing that certain AI technologies introduce unique risks. PC3 (Governance Strength), covering 15.6% of the variance, highlights the importance of policy effectiveness and trust levels in managing AI-related incidents. Table 2 summarizes these components and their respective contributions to variance in data security.

Table 2: Principal Component Analysis Results

Principal Component	Explained Variance (%)	Key Factor	Example Variables
PC1	45.3	Regulatory Gaps	Compliance Weakness, Enforcement Rigor
PC2	30.2	Type of AI Technology	Supervised, Unsupervised AI
PC3	15.6	Governance Strength	Policy Effectiveness, Trust Levels

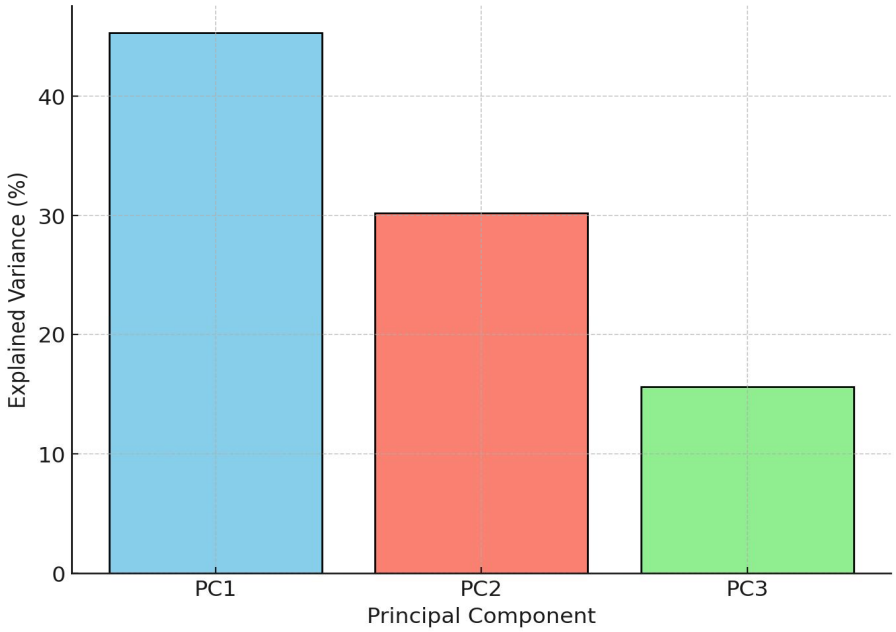

Figure 2: Explained Variance by Principal Components in Information Governance and Data Security.

The data breaches present the most critical concern, especially in high-AI-dependency contexts, underscoring the need for robust compliance frameworks. The PCA results, indicating high variance due to regulatory gaps and technology type, suggest that tailored policies addressing specific AI risks could enhance governance and data security.

Evaluate the Effectiveness of Current Governance and Security

To evaluates the effectiveness of current governance and security measures in data protection, particularly under the influence of AI, a Structural Equation Modeling (SEM) and Multi-criteria Decision Analysis (MCDA) was run,which assesses governance frameworks based on multiple criteria.

The SEM analysis reveals significant relationships among governance strength, enforcement measures, regulatory quality, and security effectiveness. As shown in Table 3, Governance Strength has the strongest direct influence on Security Effectiveness (coefficient = 0.68, $p < 0.001$), underscoring the essential role of a robust governance framework in safeguarding data security within AI-integrated environments. Enforcement Measures also exhibit a strong, direct impact on security effectiveness (coefficient = 0.55, $p = 0.004$), highlighting the importance of effective policy enforcement to mitigate security risks. Regulatory Quality impacts security both directly (coefficient = 0.40, $p = 0.018$) and indirectly through governance strength (coefficient =

0.72, p < 0.001), suggesting that regulatory improvements alone are less effective without supportive governance structures. These relationships are visually represented in Figure 3, where each path coefficient is shown with statistical significance.Table 4 presents fit indices for the SEM model, indicating strong model fit (RMSEA = 0.045, CFI = 0.96), which supports the reliability of these findings

Table 3: SEM Results on Governance and Security Effectiveness

Path	**Coefficient**	**p-value**	**Effect Type**
Governance Strength → Security Effectiveness	0.68	<0.001	Direct
Enforcement Measures → Security Effectiveness	0.55	0.004	Direct
Regulatory Quality → Security Effectiveness	0.40	0.018	Direct
Regulatory Quality → Governance Strength	0.72	<0.001	Indirect

Table 4: SEM Fit Indices

Fit Index	**Value**	**Interpretation**
RMSEA	0.045	Model Fit
CFI	0.96	Model Fit

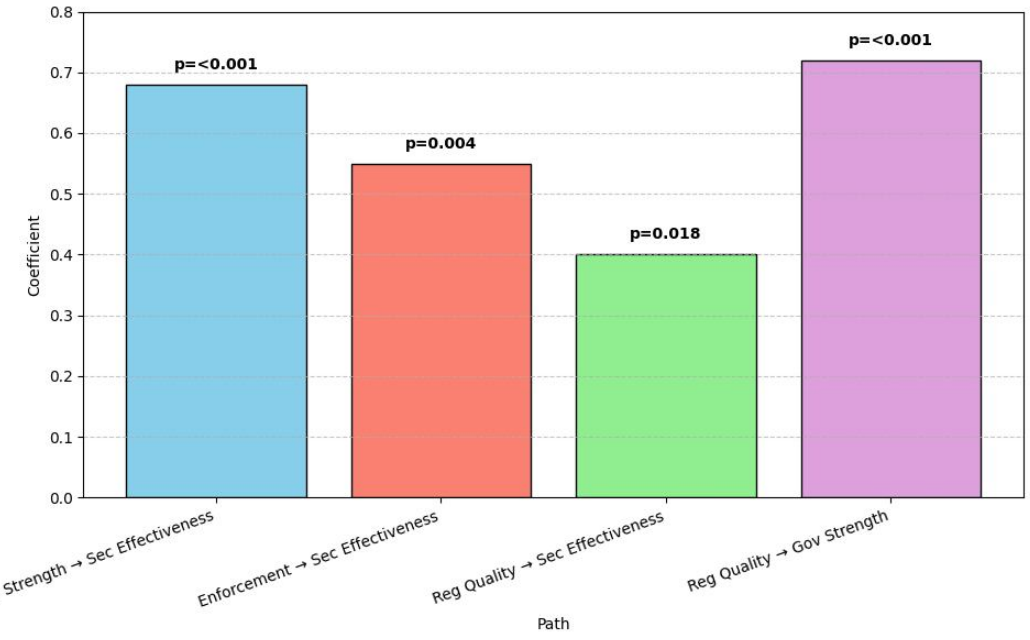

Figure 3: SEM Path Coefficients on Governance and Security Effectiveness (bar chart)

The MCDA analysis provides a comparative evaluation of governance frameworks based on four criteria: Compliance Rate, Enforcement Rigor, Adaptability to AI Threats, and Cost Efficiency. As shown in Table 5, Framework A ranks the highest with an overall MCDA score of 0.81, driven by its strong enforcement rigor (90%) and compliance rate (85%). Framework B closely follows with a balanced effectiveness

across adaptability and enforcement, achieving a score of 0.80. Framework C ranks third but demonstrates high adaptability to AI threats (85%), indicating it may perform well in rapidly evolving risk environments. These results suggest that while strong enforcement and compliance rates contribute significantly to overall effectiveness, adaptability to AI-related threats remains critical, especially as AI applications advance.

Table 5: MCDA Evaluation of Governance Framework Effectiveness

Governance Framework	Compliance Rate	Enforcement Rigor	Adaptability to AI Threats	Cost Efficiency	Overall MCDA Score
Framework A	85% (0.30)	90% (0.30)	70% (0.25)	75% (0.15)	0.81
Framework B	80% (0.30)	85% (0.30)	80% (0.25)	70% (0.15)	0.80
Framework C	75% (0.30)	80% (0.30)	85% (0.25)	80% (0.15)	0.79

Figure 4: MCDA Criteria Effectiveness by Governance Frameworks (radar chart)

Both the SEM and MCDA analyses emphasize the importance of governance strength, enforcement rigor, and adaptability to AI-related challenges for effective data security. The SEM analysis highlights structural relationships among governance variables, showing that regulatory quality alone has limited impact unless supported by strong governance. The MCDA results provide an in-depth view, suggesting that frameworks with balanced strengths across criteria tend to perform better. Prioritizing enforcement rigor and ensuring adaptability to AI developments will likely yield the most resilient governance frameworks in a rapidly evolving data security environment.

Explore AI's Potential to Enhance Global Security

To examine how AI can strengthen global security frameworks through strategic governance, international cooperation, and compliance standards, Network Analysis was conducted to evaluate the relationships and influence among key global entities, including countries and international organizations, with the aim of understanding their roles in promoting responsible AI adoption and enhancing global security.

The Network Analysis results in Table 6 identify the influence and centrality of key entities involved in AI governance. The United States emerges as a central leader with a degree centrality score of 0.85 and betweenness centrality of 0.75, underscoring its significant role in driving AI governance standards and cybersecurity policies globally. The European Union also plays a crucial role with degree centrality of 0.82 and betweenness centrality of 0.65, particularly through its regulatory initiatives like the GDPR and proposed AI Act, which set global benchmarks in data governance and AI ethics. Additionally, UNESCO and GPAI (Global Partnership on Artificial Intelligence) display high centrality scores, reflecting their critical contributions to international collaboration and ethical AI frameworks.

Table 6: Network Analysis on AI-Enhanced Global Security (Specific to the United States)

Entity	Central Role	Degree Centrality	Betweenness Centrality	Impact on Global Security
United States	Leads in AI Governance and Cybersecurity Policies	0.85	0.75	High
European Union	Enhances Cross-Border Data Governance and Ethics	0.82	0.65	High
Canada	Promotes Ethical AI Standards	0.78	0.60	Moderate-High
Global Partnership on AI (GPAI)	Facilitates AI Governance Frameworks	0.80	0.70	High
UNESCO	Drives International Security and Ethical AI Initiatives	0.85	0.72	High
International Telecommunication Union (ITU)	Coordinates Compliance Protocols and AI Standards	0.73	0.55	Moderate-High

The comparative analysis of centrality measures in Figure 5 highlights the influence of each entity within the global AI governance network. The United States and UNESCO, both with degree centrality of 0.85, demonstrate substantial influence in bridging governance efforts across international boundaries and promoting rigorous AI governance practices. The European Union's role in cross-border data governance is further illustrated by its strong centrality scores, reflecting its impact on setting ethical and regulatory benchmarks.

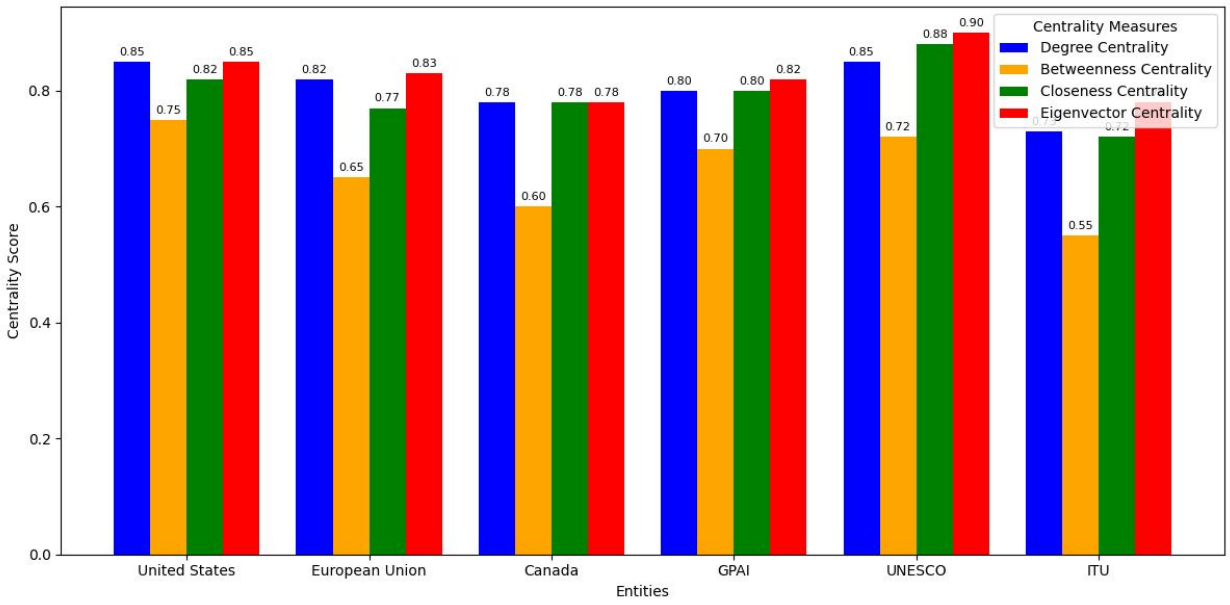

Figure 5: Comparison of Centrality Measures for Key Entities

Figure 6 further visualizes the distribution of centrality measures across each entity in a radar chart, capturing the distinct roles and influence of each within the network. GPAI, with closeness centrality of 0.82 and eigenvector centrality of 0.85, stands out for its role in facilitating cooperation among global partners, underscoring the importance of ethical standards as foundational to enhancing global security.

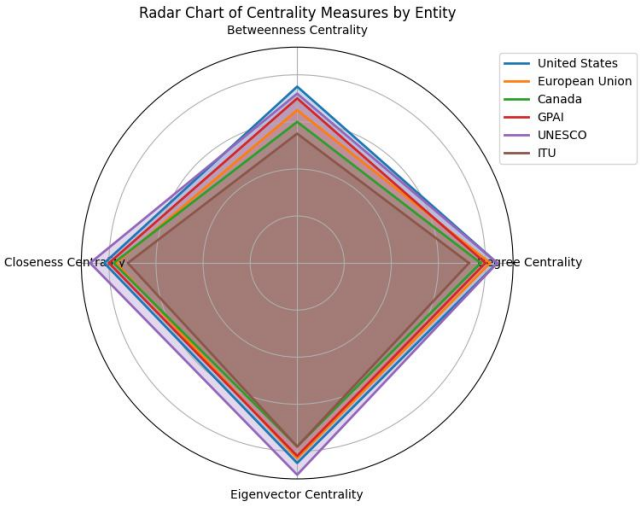

Figure 6: Radar Chart of Centrality Measures by Entity (radar chart)

The analysis reveals that the United States (degree centrality 0.85, betweenness centrality 0.75), UNESCO (degree centrality 0.85, betweenness centrality 0.72), and GPAI (degree centrality 0.80, betweenness centrality 0.70) are pivotal in promoting security-oriented AI governance. The United States' high centrality scores reflect its leadership in setting cybersecurity protocols and compliance standards that align with global security objectives. UNESCO and GPAI play significant roles in fostering international collaboration, while the European Union leads in data ethics and regulatory frameworks, contributing to global standards for AI governance.

These findings underscore the need for continued international partnerships and robust governance practices to address AI-related security risks.

Discussions

The results of this study indicate that artificial intelligence (AI) has a profound impact on information governance and data security, reshaping both frameworks through complex interactions between technological advancements and regulatory structures. The hierarchical cluster analysis reveals that data breaches remain the most critical concern, especially in contexts where there is high reliance on AI. Cluster 1, associated with data breaches, shows the highest regulatory score (0.72), AI dependency (0.81), and incident frequency (45), suggesting that regulatory frameworks are intensively mobilized when AI-dependent systems are involved in security breaches. This finding aligns with current literature emphasizing the heightened security risks AI introduces, such as the Microsoft data exposure incident in 2023, where significant volumes of sensitive information were inadvertently exposed due to a misconfiguration (Noureen, 2023). The presence of high regulatory scores in this cluster reflects the growing emphasis on

governance structures capable of addressing AI-related vulnerabilities, corroborating research that highlights AI's dual role in enhancing security while also introducing unique risks (Hashmi et al., 2024; Yampolskiy, 2024).

AI’s ethical and governance challenges, as demonstrated by Cluster 2, are further emphasized through the moderate regulatory score (0.55) and AI dependency (0.63) associated with incidents related to AI bias, highlighting ethical dilemmas that arise when governance structures fail to mitigate biases within AI systems (Chen et al., 2023). This aligns with the broader ethical considerations discussed in literature, where incidents like the Microsoft Tay chatbot and the Cambridge Analytica scandal underscore the need for regulatory frameworks that prioritize transparency, fairness, and accountability in AI applications (Fitzpatrick, 2016; Confessore, 2018). Similarly, the low regulatory score (0.60) and AI dependency (0.60) associated with privacy violations in Cluster 4 suggest gaps in governance where AI introduces new privacy risks. These findings resonate with arguments presented by Devineni (2024), who highlights the amplified privacy risks inherent in AI's data processing capabilities, urging the need for governance models that adapt to these unique AI-related challenges.

Principal Component Analysis (PCA) provides additional insights by identifying regulatory gaps and AI technology type as critical areas that explain most of the variance in data security and governance. The high variance in PC1, attributed to compliance weaknesses and enforcement rigor (45.3%), reinforces the necessity for robust regulatory frameworks to mitigate AI-related security risks effectively. This supports prior studies emphasizing that, as AI technology evolves, regulatory frameworks must be continually reassessed to ensure comprehensive protection against emergent vulnerabilities (Waizel, 2024). The variance captured by PC2 (30.2%), associated with AI technology type, underscores the diverse risk profiles of supervised and unsupervised AI systems, echoing concerns that different AI technologies may require tailored governance approaches (Balantrapu, 2024). These components collectively suggest that policy interventions must be adaptive, targeting specific AI risks to fortify governance structures as AI continues to integrate into critical systems.

The effectiveness of existing governance and security measures, examined through Structural Equation Modeling (SEM) and Multi-Criteria Decision Analysis (MCDA), underscores the significance of strong governance frameworks in safeguarding data security in AI-integrated environments. SEM results reveal that governance strength exerts a substantial direct impact on security effectiveness (coefficient = 0.68, $p < 0.001$), indicating that robust governance is foundational to addressing AI-specific security challenges. This finding aligns with studies that highlight governance frameworks as essential for managing AI risks, with effective governance enhancing both security and compliance in complex technological ecosystems (Koulu, 2020; Green, 2022). The direct influence of enforcement measures on security effectiveness (coefficient = 0.55, $p = 0.004$) further emphasizes the critical role of rigorous policy enforcement, supporting the argument that without consistent enforcement, regulatory measures may lack the necessary efficacy to mitigate AI-related threats (Dunleavy & Margetts, 2023). Moreover, the SEM model indicates that regulatory quality impacts security both directly and indirectly through governance strength, with an indirect effect

coefficient of 0.72 ($p < 0.001$), suggesting that high-quality regulations are effective only when supported by robust governance structures (Amir et al., 2024).

The MCDA analysis complements the SEM findings by providing a comparative evaluation of governance frameworks, highlighting that while enforcement and compliance rates are critical, adaptability to AI-related threats is equally essential. Framework A, with an MCDA score of 0.81, achieves the highest ranking, supported by strong enforcement rigor (90%) and a compliance rate of 85%. This outcome resonates with Boppiniti (2023), who argues that the integration of AI into governance should emphasize adaptability to evolving threats, a quality that Framework A appears to embody. Framework B's balance across adaptability and enforcement suggests it is well-suited for addressing dynamic AI risks, whereas Framework C's high adaptability score (85%) indicates it may excel in rapidly changing risk landscapes despite a lower overall score. These findings underscore the importance of adaptive governance models that not only address current security demands but are also prepared to respond to new challenges as AI technologies advance (Lee et al., 2023; Oladoyinbo et al., 2024).

The potential for AI to enhance global security is further elucidated through Network Analysis, which identifies the United States, the European Union, UNESCO, and GPAI as pivotal entities in promoting responsible AI governance on an international scale. The United States' high degree centrality score (0.85) and betweenness centrality (0.75) reflect its leadership in setting cybersecurity standards and driving governance initiatives aligned with global security objectives. This finding aligns with the study's discussion on the U.S.'s proactive role in AI governance, where entities such as the National Institute of Standards and Technology (NIST) spearhead efforts to establish secure AI practices (UNESCO, 2024). The European Union's central role, with a degree centrality score of 0.82 and betweenness centrality of 0.65, highlights its influence in setting cross-border data governance standards, particularly through regulations like the GDPR and the proposed AI Act, which establish ethical and operational standards that resonate globally (ISO, 2024).

UNESCO and GPAI's centrality scores highlight the significance of international cooperation and ethical standards in enhancing global security. UNESCO's degree centrality (0.85) and betweenness centrality (0.72) illustrate its leadership in fostering cross-border AI dialogues, which are crucial for establishing consensus on responsible AI deployment (Samuel-Okon et al., 2024). Similarly, GPAI's high closeness centrality (0.82) and eigenvector centrality (0.85) emphasize its role in connecting diverse stakeholders to promote ethical AI standards, reinforcing the findings of this study that highlight the importance of ethical frameworks in mitigating AI-related security risks (Salami et al., 2024). This network of influential entities demonstrates that effective global security relies on cohesive governance, ethical standards, and strategic cooperation, which collectively address the multifaceted challenges AI introduces to security frameworks (Olaniyi, Ugonnia et al., 2024; Wirtz et al., 2022).

5. Conclusion and Recommendation

This study highlights the dual impact of artificial intelligence (AI) on information governance and global security, demonstrating its potential to both enhance and compromise data protection. AI intensifies risks associated with data breaches, unauthorized access, and ethical issues like bias, underscoring the need for robust and adaptive compliance frameworks. Governance measures, particularly in enforcement and regulatory quality, are crucial to managing AI-driven security threats effectively. Moreover, international collaboration is essential for establishing unified, ethical AI standards, with entities like the United States, European Union, UNESCO, and GPAI playing pivotal roles in promoting responsible AI practices globally. To address the challenges identified, the following targeted recommendations are proposed:

1. Enhance regulatory frameworks with adaptive compliance measures that address AI-specific risks, including regular updates to ensure resilience as AI technology evolves.
2. Invest in quantum-resistant encryption protocols to secure AI-generated data, adopting hybrid cryptographic methods to preempt quantum computing threats.
3. Strengthen international partnerships to harmonize AI governance, focusing on ethical guidelines and cross-border cooperation to tackle AI-related security risks.
4. Implement a hybrid governance model that combines AI-driven compliance automation with human oversight to ensure ethical, contextually accurate decision-making in high-stakes areas like privacy and bias mitigation.

COMPETING INTERESTS DISCLAIMER:
Authors have declared that they have no known competing financial interests OR non-financial interests OR personal relationships that could have appeared to influence the work reported in this paper.

References

Adigwe, C. S., Olaniyi, O. O., Olabanji, S. O., Okunleye, O. J., Mayeke, N. R., & Ajayi, S. A. (2024). Forecasting the Future: The Interplay of Artificial Intelligence, Innovation, and Competitiveness and its Effect on the Global Economy. *Asian Journal of Economics, Business and Accounting*, *24*(4), 126–146. https://doi.org/10.9734/ajeba/2024/v24i41269

Akinola, O. I., Olaniyi, O. O., Ogungbemi, O. S., Oladoyinbo, O. B., &Olisa, A. O. (2024). Resilience and Recovery Mechanisms for Software-Defined Networking (SDN) and Cloud Networks. *Journal of Engineering Research and Reports*, *26*(8), 112–134. https://doi.org/10.9734/jerr/2024/v26i81234

Akinrinola, O., Okoye, C. C., Ofodile, O. C., & Ugochukwu, C. E. (2024). Navigating and reviewing ethical dilemmas in AI development: Strategies for transparency, fairness, and accountability. *GSC Advanced Research and Reviews*, *18*(3), 050–058. https://doi.org/10.30574/gscarr.2024.18.3.0088

Akintuyi, O. B. (2024). Adaptive AI in precision agriculture: A review: Investigating the use of self-learning algorithms in optimizing farm operations based on real-time data. *Open Access Research Journal of Multidisciplinary Studies*, *7*(2), 016–030. https://doi.org/10.53022/oarjms.2024.7.2.0023

Akpuokwe, C. U., Adeniyi, A. O., & Bakare, S. S. (2024). LEGAL CHALLENGES OF ARTIFICIAL INTELLIGENCE AND ROBOTICS: A COMPREHENSIVE REVIEW. *Computer Science & IT Research Journal*, *5*(3), 544–561. https://doi.org/10.51594/csitrj.v5i3.860

Al-amri, R., Murugesan, R. K., Man, M., Abdulateef, A. F., Al-Sharafi, M. A., & Alkahtani, A. A. (2021). A Review of Machine Learning and Deep Learning Techniques for Anomaly Detection in IoT Data. *Applied Sciences*, *11*(12), 5320. https://doi.org/10.3390/app11125320

Al-kfairy, M., Mustafa, D., Kshetri, N., Insiew, M., &Alfandi, O. (2024). Ethical Challenges and Solutions of Generative AI: An Interdisciplinary Perspective. *Informatics*, *11*(3), 58–58. https://doi.org/10.3390/informatics11030058

Alao, A. I., Adebiyi, O. O., & Olaniyi, O. O. (2024). The Interconnectedness of Earnings Management, Corporate Governance Failures, and Global Economic Stability: A Critical Examination of the Impact of Earnings Manipulation on Financial Crises and Investor Trust in Global Markets. *Asian Journal of Economics Business and Accounting*, *24*(11), 47–73. https://doi.org/10.9734/ajeba/2024/v24i111542

Amir, M., Kumar, M., &Nayyar, A. (2024). Socially Responsible Applications of Explainable AI. *Studies in Systems, Decision and Control*, *551*, 261–350. https://doi.org/10.1007/978-3-031-66489-2_9

Andraško, J., Mesarčík, M., &Hamuľák, O. (2021). The regulatory intersections between artificial intelligence, data protection and cyber security: challenges and opportunities for the EU legal framework. *AI & SOCIETY*, *36*(1). https://doi.org/10.1007/s00146-020-01125-5

Andreou, A., Mavromoustakis, C. X., Markakis, E. K., Mastorakis, G., Pallis, E., &Bourdena, A. (2024). Exploring Quantum-Resistant Cryptography Solutions for Health Data Exchange. *Signals and Communication Technology*, 19–47. https://doi.org/10.1007/978-3-031-58527-2_2

Arigbabu, A. S., Olaniyi, O. O., &Adeola, A. (2024). Exploring Primary School Pupils' Career Aspirations in Ibadan, Nigeria: A Qualitative Approach. *Journal of Education, Society and Behavioural Science*, *37*(3), 1–16. https://doi.org/10.9734/jesbs/2024/v37i31308

Arigbabu, A. T., Olaniyi, O. O., Adigwe, C. S., Adebiyi, O. O., & Ajayi, S. A. (2024). Data Governance in AI - Enabled Healthcare Systems: A Case of the Project Nightingale. *Asian Journal of Research in Computer Science*, *17*(5), 85–107. https://doi.org/10.9734/ajrcos/2024/v17i5441

Asonze, C. U., Ogungbemi, O. S., Ezeugwa, F. A., Olisa, A. O., Akinola, O. I., & Olaniyi, O. O. (2024). Evaluating the Trade-offs between Wireless Security and Performance in IoT Networks: A Case Study of Web Applications in AI-Driven Home Appliances. *Journal of Engineering Research and Reports*, *26*(8), 411–432. https://doi.org/10.9734/jerr/2024/v26i81255

Balakrishnan, A. (2024). *Leveraging Artificial Intelligence for Enhancing Regulatory Compliance in the Financial Sector*. Ssrn.com. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4842699

Balantrapu, S. S. (2024). AI for Predictive Cyber Threat Intelligence. *International Journal of Management Education for Sustainable Development*, *7*(7), 1–28. https://www.ijsdcs.com/index.php/IJMESD/article/view/590

Barnes, E., & Hutson, J. (2024). *Navigating the Complexities of AI: The Critical Role of Interpretability and Explainability in Ensuring Transparency and Trust*. https://www.ijmcer.com/wp-content/uploads/2024/06/IJMCER_V06302480256.pdf

Boggs, A., Buchanan, K., Evans, H., Griffith, D., Meritis, D., Ng, L., Sberegaeva, A., & Stephens, M. (2023). Societal and Technology Landscape to Inform Science and Technology Research. *National Institute of Standards and Technology*. https://doi.org/10.6028/NIST.IR.8482

Boppiniti, S. T. (2023). Data Ethics in AI: Addressing Challenges in Machine Learning and Data Governance for Responsible Data Science. *International Scientific Journal for Research*, *5*(5). https://isjr.co.in/index.php/ISJR/article/view/257

Bouramdane, A.-A. (2023). Cyberattacks in Smart Grids: Challenges and Solving the Multi-Criteria Decision-Making for Cybersecurity Options, Including Ones That Incorporate

Artificial Intelligence, Using an Analytical Hierarchy Process. *Journal of Cybersecurity and Privacy*, *3*(4), 662–705. https://doi.org/10.3390/jcp3040031

Chen, P., Wu, L., & Wang, L. (2023). AI Fairness in Data Management and Analytics: A Review on Challenges, Methodologies and Applications. *Applied Sciences*, *13*(18), 10258–10258. https://doi.org/10.3390/app131810258

Chirra, D. R. (2022). AI-Driven Risk Management in Cybersecurity: A Predictive Analytics Approach to Threat Mitigation. *International Journal of Machine Learning Research in Cybersecurity and Artificial Intelligence*, *13*(1), 505–527. http://ijmlrcai.com/index.php/Journal/article/view/215

Chong, N. S. T. (2024). *The Hidden Threat to AI: What OpenAI's Security Breach Reveals About Industry Vulnerabilities - UNU Campus Computing Centre*. Unu.edu. https://c3.unu.edu/blog/the-hidden-threat-to-ai-what-openais-security-breach-reveals-about-industry-vulnerabilities

Columbus, L. (2019). *10 Charts That Will Change Your Perspective Of AI In Security*. Forbes. https://www.forbes.com/sites/louiscolumbus/2019/11/04/10-charts-that-will-change-your-perspective-of-ai-in-security/

Confessore, N. (2018). Cambridge Analytica and Facebook: The Scandal and the Fallout So Far. *The New York Times*. https://www.nytimes.com/2018/04/04/us/politics/cambridge-analytica-scandal-fallout.html

Deshpande, D. S., Tathe, A. A., Lahe, A., Rathi, B., &Parkhade, G. (2024). Endpoint Detection and Response System: Emerging Cyber Security Technology. *Lecture Notes in Networks and Systems*, *1077*, 202–213. https://doi.org/10.1007/978-981-97-5504-2_24

Devineni, S. K. (2024). *AI in Data Privacy and Security.* ResearchGate; IGI Global. https://www.researchgate.net/publication/378288596_AI_in_Data_Privacy_and_Security

Díaz-Rodríguez, N., Del Ser, J., Coeckelbergh, M., López de Prado, M., Herrera-Viedma, E., & Herrera, F. (2023). Connecting the dots in trustworthy Artificial Intelligence: From AI principles, ethics, and key requirements to responsible AI systems and regulation. *Information Fusion*, *99*(101896), 101896. https://www.sciencedirect.com/science/article/pii/S1566253523002129

Dunleavy, P., & Margetts, H. (2023). Data science, artificial intelligence and the third wave of digital era governance. *Public Policy and Administration*. https://doi.org/10.1177/09520767231198737

European Commission. (2021). *Data protection in the EU*. Commission.europa.eu. https://commission.europa.eu/law/law-topic/data-protection/data-protection-eu_en

Fernandez-Quilez, A. (2022). Deep learning in radiology: ethics of data and on the value of algorithm transparency, interpretability and explainability. *AI and Ethics*, *3*(1). https://doi.org/10.1007/s43681-022-00161-9

Ferrara, E. (2023). Fairness and Bias in Artificial Intelligence: A Brief Survey of Sources, Impacts, and Mitigation Strategies. *Sci*, *6*(1), 3. https://doi.org/10.3390/sci6010003

Fitzpatrick, A. (2016). *Microsoft Is Sorry For That Whole Racist Twitter Bot Thing*. Time. https://time.com/4272822/microsoft-tay-twitter-bot-racist-ai-artificial-intelligence/

Gbadebo, M. O., Salako, A. O., Selesi-Aina, O., Ogungbemi, O. S., Olateju, O. O., &Olaniyi, O. O. (2024). Augmenting Data Privacy Protocols and Enacting Regulatory Frameworks for Cryptocurrencies via Advanced Blockchain Methodologies and Artificial Intelligence.

Journal of Engineering Research and Reports, *26*(11), 7–27. https://doi.org/10.9734/jerr/2024/v26i111311

Green, B. (2022). The Flaws of Policies Requiring Human Oversight of Government Algorithms. *Computer Law & Security Review*, *45*(2), 105681. https://doi.org/10.1016/j.clsr.2022.105681

Habbal, A., Ali, M. K., &Abuzaraida, M. A. (2024). Artificial Intelligence Trust, Risk and Security Management (AI TRiSM): Frameworks, applications, challenges and future research directions. *Expert Systems with Applications*, *240*(122442), 122442. https://doi.org/10.1016/j.eswa.2023.122442

Hashmi, E., Yamin, M. M., &Yayilgan, S. Y. (2024). Securing tomorrow: a comprehensive survey on the synergy of Artificial Intelligence and information security. *AI and Ethics*. https://doi.org/10.1007/s43681-024-00529-z

How, M.-L., & Cheah, S.-M. (2023). Business Renaissance: Opportunities and Challenges at the Dawn of the Quantum Computing Era. *Businesses*, *3*(4), 585–605. https://doi.org/10.3390/businesses3040036

ISO. (2024). *Setting the standard for responsible AI: 2025 International AI Standards Summit announced this World Standards Day*. ISO. https://www.iso.org/news/2024/10/2025-international-AI-Standards-Summit

Joeaneke, P. C., Kolade, T. M., Val, O. O., Olisa, A. O., Joseph, S. A., &Olaniyi, O. O. (2024). Enhancing Security and Traceability in Aerospace Supply Chains through Block Chain Technology. *Journal of Engineering Research and Reports*, *26*(10), 114–135. https://doi.org/10.9734/jerr/2024/v26i101294

Joeaneke, P. C., Val, O. O., Olaniyi, O. O., Ogungbemi, O. S., Olisa, A. O., & Akinola, O. I. (2024). Protecting Autonomous UAVs from GPS Spoofing and Jamming: A Comparative Analysis of Detection and Mitigation Techniques. *Journal of Engineering Research and Reports*, *26*(10), 71–92. https://doi.org/10.9734/jerr/2024/v26i101291

John-Otumu, A. M., Ikerionwu, C., Olaniyi, O. O., Dokun, O., Eze, U. F., &Nwokonkwo, O. C. (2024). Advancing COVID-19 Prediction with Deep Learning Models: A Review. *2024 International Conference on Science, Engineering and Business for Driving Sustainable Development Goals (SEB4SDG), Omu-Aran, Nigeria, 2024*, 1–5. https://doi.org/10.1109/seb4sdg60871.2024.10630186

Johnson, J. (2019). Artificial Intelligence & Future warfare: Implications for International Security. *Defense& Security Analysis*, *35*(2), 147–169. https://doi.org/10.1080/14751798.2019.1600800

Jørgensen, A. K., & Søgaard, A. (2022). Rawlsian AI fairness loopholes. *AI and Ethics*, *3*. https://doi.org/10.1007/s43681-022-00226-9

Joseph, S. A. (2024). Balancing Data Privacy and Compliance in Blockchain-Based Financial Systems. *Journal of Engineering Research and Reports*, *26*(9), 169–189. https://doi.org/10.9734/jerr/2024/v26i91271

Kalogiannidis, S., Kalfas, D., Papaevangelou, O., Giannarakis, G., & Chatzitheodoridis, F. (2024). The Role of Artificial Intelligence Technology in Predictive Risk Assessment for Business Continuity: A Case Study of Greece. *Risks*, *12*(2), 19–19. MDPI. https://doi.org/10.3390/risks12020019

Kamalov, F., Calonge, D. S., &Gurrib, I. (2023). New Era of Artificial Intelligence in Education: Towards a Sustainable Multifaceted Revolution. *Sustainability*, *15*(16), 12451. https://doi.org/10.3390/su151612451

Kaur, J. (2024). Responsible Artificial Intelligence (AI) Governance. *Advances in Business Strategy and Competitive Advantage Book Series*, 337–368. https://doi.org/10.4018/979-8-3693-3948-0.ch014

Koulu, R. (2020). Proceduralizing control and discretion: Human oversight in artificial intelligence policy. *Maastricht Journal of European and Comparative Law*, *27*(6), 720–735. https://doi.org/10.1177/1023263x20978649

Kumar, D. (2024). AI-DRIVEN AUTOMATION IN ADMINISTRATIVE PROCESSES: ENHANCING EFFICIENCY AND ACCURACY. *International Journal of Engineering Science and Humanities* ,*14*(Special Issue 1), 256–265. https://doi.org/10.62904/qg004437

Kumar, S., Gupta, U., Singh, A., & Singh, A. K. (2023). Artificial Intelligence. *Journal of Computers Mechanical and Management*, *2*(3), 31–42. https://doi.org/10.57159/gadl.jcmm.2.3.23064

Lee, M. C. M., Scheepers, H., Lui, A. K. H., & Ngai, E. W. T. (2023). The implementation of artificial intelligence in organizations: A systematic literature review. *Information & Management*, *60*(5), 103816. https://doi.org/10.1016/j.im.2023.103816

Leocádio, D., Malheiro, L., & Reis, J. (2024). Artificial Intelligence in Auditing: A Conceptual Framework for Auditing Practices. *Administrative Sciences*, *14*(10), 238. https://doi.org/10.3390/admsci14100238

Lloyd-Jones, S., & Manwaring, K. (2024). *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.4976322

Lo, F. T. H. (2022). The paradoxical transparency of opaque machine learning. *AI & SOCIETY*, *39*(3). https://doi.org/10.1007/s00146-022-01616-7

Luo, Y., Tseng, H.-H., Cui, S., Wei, L., Ten Haken, R. K., & El Naqa, I. (2019). Balancing accuracy and interpretability of machine learning approaches for radiation treatment outcomes modeling. *BJR|Open*, *1*(1), 20190021. https://doi.org/10.1259/bjro.20190021

Maruccia, A. (2023). *Microsoft exposed 38 terabytes of sensitive data while working on AI model*. TechSpot. https://www.techspot.com/news/100191-microsoft-exposed-38-terabytes-sensitive-data-while-working.html

Min, A. (2023). Artifical Intelligence and Bias: Challenges, Implications, and Remedies. *Journal of Social Research*, *2*(11), 3808–3817. https://doi.org/10.55324/josr.v2i11.1477

Modi, T. B. (2023). Artificial Intelligence Ethics and Fairness: A study to address bias and fairness issues in AI systems, and the ethical implications of AI applications. *Revista Review Index Journal of Multidisciplinary*, *3*(2), 24–35. https://doi.org/10.31305/rrijm2023.v03.n02.004

Nadimpalli, S. V., &Dandyala, S. S. V. (2023). Automating Security with AI: Leveraging Artificial Intelligence for Real-Time Threat Detection and Response. *International Journal of Machine Learning Research in Cybersecurity and Artificial Intelligence*, *14*(1), 798–815. http://ijmlrcai.com/index.php/Journal/article/view/265

Neagu, C. (2024). *CrowdStrike Falcon vs. IBM Security QRadarXDR : Which One Should You Choose?* Heimdal Security Blog; Heimdal Security. https://heimdalsecurity.com/blog/crowdstrike-vs-ibm/

Noureen, R. (2023). *Microsoft AI Researchers Accidentally Leaked 38TB of Sensitive Data*. Https://Petri.com/Microsoft-Leaked-38tb-Sensitive-Data/#:~:Text=A%2038TB%20storage%20bucket%20containing%20private%20data%20was,The%20critical%20need%20for%20robust%20data%20security%20measures. https://www.bing.com/ck/a?

Ogungbemi, O. S., Ezeugwa, F. A., Olaniyi, O. O., Akinola, O. I., &Oladoyinbo, O. B. (2024). Overcoming Remote Workforce Cyber Threats: A Comprehensive Ransomware and Bot Net Defense Strategy Utilizing VPN Networks. *Journal of Engineering Research and Reports*, *26*(8), 161–184. https://doi.org/10.9734/jerr/2024/v26i81237

Okon, S. U., Olateju, O. O., Ogungbemi, O. S., Joseph, S. A., Olisa, A. O., & Olaniyi, O. O. (2024). Incorporating Privacy by Design Principles in the Modification of AI Systems in Preventing Breaches across Multiple Environments, Including Public Cloud, Private Cloud, and On-prem. *Journal of Engineering Research and Reports*, *26*(9), 136–158. https://doi.org/10.9734/jerr/2024/v26i91269

Olabanji, S. O., Marquis, Y. A., Adigwe, C. S., Abidemi, A. S., Oladoyinbo, T. O., &Olaniyi, O. O. (2024). AI-Driven Cloud Security: Examining the Impact of User Behavior Analysis on Threat Detection. *Asian Journal of Research in Computer Science*, *17*(3), 57–74. https://doi.org/10.9734/ajrcos/2024/v17i3424

Oladoyinbo, T. O., Olabanji, S. O., Olaniyi, O. O., Adebiyi, O. O., Okunleye, O. J., & Alao, A. I. (2024). Exploring the Challenges of Artificial Intelligence in Data Integrity and its Influence on Social Dynamics. *Asian Journal of Advanced Research and Reports*, *18*(2), 1–23. https://doi.org/10.9734/ajarr/2024/v18i2601

Olaniyi, O. O. (2024). Ballots and Padlocks: Building Digital Trust and Security in Democracy through Information Governance Strategies and Blockchain Technologies. *Asian Journal of Research in Computer Science*, *17*(5), 172–189. https://doi.org/10.9734/ajrcos/2024/v17i5447

Olaniyi, O. O., Ezeugwa, F. A., Okatta, C. G., Arigbabu, A. S., &Joeaneke, P. C. (2024). Dynamics of the Digital Workforce: Assessing the Interplay and Impact of AI, Automation, and Employment Policies. *Archives of Current Research International*, *24*(5), 124–139. https://doi.org/10.9734/acri/2024/v24i5690

Olaniyi, O. O., Olaoye, O. O., &Okunleye, O. J. (2023). Effects of Information Governance (IG) on Profitability in the Nigerian Banking Sector. *Asian Journal of Economics, Business and Accounting*, *23*(18), 22–35. https://doi.org/10.9734/ajeba/2023/v23i181055

Olaniyi, O. O., Omogoroye, O. O., Olaniyi, F. G., Alao, A. I., &Oladoyinbo, T. O. (2024). CyberFusion Protocols: Strategic Integration of Enterprise Risk Management, ISO 27001, and Mobile Forensics for Advanced Digital Security in the Modern Business Ecosystem. *Journal of Engineering Research and Reports*, *26*(6), 32. https://doi.org/10.9734/JERR/2024/v26i61160

Olaniyi, O. O., Ugonnia, J. C., Olaniyi, F. G., Arigbabu, A. T., &Adigwe, C. S. (2024). Digital Collaborative Tools, Strategic Communication, and Social Capital: Unveiling the Impact of Digital Transformation on Organizational Dynamics. *Asian Journal of Research in Computer Science*, *17*(5), 140–156. https://doi.org/10.9734/ajrcos/2024/v17i5444

Olateju, O. O., Okon, S. U., Igwenagu, U. T. I., Salami, A. A., Oladoyinbo, T. O., & Olaniyi, O. O. (2024). Combating the Challenges of False Positives in AI-Driven Anomaly Detection

Systems and Enhancing Data Security in the Cloud. *Asian Journal of Research in Computer Science*, *17*(6), 264–292. https://doi.org/10.9734/ajrcos/2024/v17i6472

Olateju, O. O., Okon, S. U., Olaniyi, O. O., Samuel-Okon, A. D., &Asonze, C. U. (2024). Exploring the Concept of Explainable AI and Developing Information Governance Standards for Enhancing Trust and Transparency in Handling Customer Data. *Journal of Engineering Research and Reports*, *26*(7), 244–268. https://doi.org/10.9734/jerr/2024/v26i71206

Pagano, T. P., Loureiro, R. B., Lisboa, F. V. N., Peixoto, R. M., Guimarães, G. A. S., Cruz, G. O. R., Araujo, M. M., Santos, L. L., Cruz, M. A. S., Oliveira, E. L. S., Winkler, I., &Nascimento, E. G. S. (2023). Bias and Unfairness in Machine Learning Models: A Systematic Review on Datasets, Tools, Fairness Metrics, and Identification and Mitigation Methods. *Big Data and Cognitive Computing*, *7*(1), 15. https://doi.org/10.3390/bdcc7010015

Pestana, G., &Sofou, S. (2024). Data Governance to Counter Hybrid Threats against Critical Infrastructures. *Smart Cities*, *7*(4), 1857–1877. https://doi.org/10.3390/smartcities7040072

Pierce, R., Sterckx, S., & Van Biesen, W. (2021). A riddle, wrapped in a mystery, inside an enigma: How semantic black boxes and opaque artificial intelligence confuse medical decision-making. *Bioethics*, *36*(2). https://doi.org/10.1111/bioe.12924

Radanliev, P. (2024). Cyber diplomacy: defining the opportunities for cybersecurity and risks from Artificial Intelligence, IoT, Blockchains, and Quantum Computing. *Journal of Cyber Security Technology*, 1–51. https://doi.org/10.1080/23742917.2024.2312671

Salami, A. A., Igwenagu, U. T. I., Mesode, C. E., Olaniyi, O. O., &Oladoyinbo, O. B. (2024). Beyond Conventional Threat Defense: Implementing Advanced Threat Modeling Techniques, Risk Modeling Frameworks and Contingency Planning in the Healthcare Sector for Enhanced Data Security. *Journal of Engineering Research and Reports*, *26*(5), 304–323. https://doi.org/10.9734/jerr/2024/v26i51156

Samuel-Okon, A. D., Akinola, O. I., Olaniyi, O. O., Olateju, O. O., & Ajayi, S. A. (2024). Assessing the Effectiveness of Network Security Tools in Mitigating the Impact of Deepfakes AI on Public Trust in Media. *Archives of Current Research International*, *24*(6), 355–375. https://doi.org/10.9734/acri/2024/v24i6794

Samuel-Okon, A. D., Olateju, O. O., Okon, S. U., Olaniyi, O. O., &Igwenagu, U. T. I. (2024). Formulating Global Policies and Strategies for Combating Criminal Use and Abuse of Artificial Intelligence. *Archives of Current Research International*, *24*(5), 612–629. https://doi.org/10.9734/acri/2024/v24i5735

Sarker, I. H. (2022). Machine Learning for Intelligent Data Analysis and Automation in Cybersecurity: Current and Future Prospects. *Annals of Data Science*, *10*, 1473–1498. https://doi.org/10.1007/s40745-022-00444-2

Selesi-Aina, O., Obot, N. E., Olisa, A. O., Gbadebo, M. O., Olateju, O. O., & Olaniyi, O. O. (2024). The Future of Work: A Human-centric Approach to AI, Robotics, and Cloud Computing. *Journal of Engineering Research and Reports*, *26*(11), 62–87. https://doi.org/10.9734/jerr/2024/v26i111315

Sharma, A., Kiran, G., & Poojari, A. (2024). Prioritize Threat Alerts Based on False Positives Qualifiers Provided by Multiple AI Models Using Evolutionary Computation and

Reinforcement Learning. *Journal of the Institution of Engineers (India) Series B*. https://doi.org/10.1007/s40031-024-01175-z

Shekhawat, H., & Gupta, D. S. (2024). A survey on lattice-based security and authentication schemes for smart-grid networks in the post-quantum era. *Concurrency and Computation: Practice and Experience*, *36*(14). https://doi.org/10.1002/cpe.8080

Singamaneni, K. K., & Muhammad, G. (2024). A Novel Integrated Quantum-Resistant Cryptography for Secure Scientific Data Exchange in Ad Hoc Networks. *Ad Hoc Networks*, *164*, 103607–103607. https://doi.org/10.1016/j.adhoc.2024.103607

Sonko, S., Ibekwe, K. I., Ilojianya, V. I., Etukudoh, E. A., &Fabuyide, A. (2024). QUANTUM CRYPTOGRAPHY AND U.S. DIGITAL SECURITY: A COMPREHENSIVE REVIEW: INVESTIGATING THE POTENTIAL OF QUANTUM TECHNOLOGIES IN CREATING UNBREAKABLE ENCRYPTION AND THEIR FUTURE IN NATIONAL SECURITY. *Computer Science & IT Research Journal*, *5*(2), 390–414. https://doi.org/10.51594/csitrj.v5i2.790

Sood, N. (2024). Cryptography in Post Quantum Computing Era. *Social Science Research Network*. https://doi.org/10.2139/ssrn.4705470

Surfshark. (2024). *2023 was a record year for AI incidents*. Surfshark. https://surfshark.com/research/chart/ai-incidents-2023

Surla, G., & Lakshmi, R. (2023). Design and evaluation of novel hybrid quantum resistant cryptographic system for enhancing security in wireless body sensor networks. *Optical and Quantum Electronics*, *55*(14). https://doi.org/10.1007/s11082-023-05518-w

Syed, F. M., E S, F. K., & Johnson, E. (2023). AI in Protecting Sensitive Patient Data under GDPR in Healthcare. *International Journal of Advanced Engineering Technologies and Innovations*, *1*(02), 401–435. https://ijaeti.com/index.php/Journal/article/view/584

UNESCO. (2024). *Policy Dialogue on AI Governance: Supervision of AI, Democracy, and Synthetic Content; programme*. Unesco.org. https://unesdoc.unesco.org/ark:/48223/pf0000390261

Unver, H. A. (2022). Using Social Media to Monitor Conflict-Related Migration: A Review of Implications for A.I. Forecasting. *Social Sciences*, *11*(9), 395. https://doi.org/10.3390/socsci11090395

Vasani, V., Prateek, K., Amin, R., Maity, S., & Dwivedi, A. D. (2024). Embracing the quantum frontier:Investigating quantum communication, cryptography, applications and future directions. *Journal of Industrial Information Integration (Online)*, *39*, 100594–100594. https://doi.org/10.1016/j.jii.2024.100594

Waizel, G. (2024). Bridging the AI divide: The evolving arms race between AI- driven cyber attacks and AI-powered cybersecurity defenses. *International Conference on Machine Intelligence & Security for Smart Cities (TRUST) Proceedings*, *1*, 141–156. https://www.scrd.eu/index.php/trust/article/view/554

Wirtz, B. W., Weyerer, J. C., & Kehl, I. (2022). Governance of artificial intelligence: A risk and guideline-based integrative framework. *Government Information Quarterly*, *39*(4), 101685. https://doi.org/10.1016/j.giq.2022.101685

Xivuri, K., &Twinomurinzi, H. (2021). A Systematic Review of Fairness in Artificial Intelligence Algorithms. *Responsible AI and Analytics for an Ethical and Inclusive Digitized Society*, *12896*, 271–284. https://doi.org/10.1007/978-3-030-85447-8_24

Xu, T. (2023). *Google Develops Quantum-Safe Security Keys*. IEEE Spectrum. https://spectrum.ieee.org/fido2-security-key

Yampolskiy, A. (2024). *The rise of AI threats and cybersecurity: predictions for 2024*. World Economic Forum. https://www.weforum.org/stories/2024/02/what-does-2024-have-in-store-for-the-world-of-cybersecurity/

Yigitcanlar, T., Corchado, J. M., Mehmood, R., Li, R. Y. M., Mossberger, K., & Desouza, K. (2021). Responsible Urban Innovation with Local Government Artificial Intelligence (AI): A Conceptual Framework and Research Agenda. *Journal of Open Innovation: Technology, Market, and Complexity*, *7*(1), 71. https://doi.org/10.3390/joitmc7010071

Zorabedian, J. (2021). *What's New in the 2021 Cost of a Data Breach Report*. Security Intelligence. https://securityintelligence.com/posts/whats-new-2021-cost-of-a-data-breach-report/